I SISTEMI INTEGRATI DI SICUREZZA PER LA PROTEZIONE DEI BENI CULTURALI

Fabio Garzia
Ingegneria della Sicurezza - DICMMPM
Università degli Studi di Roma "La Sapienza"
Via Eudossiana, 18 - 00184 Roma
tel. 0644585626, fax 06233207150, email fabio.garzia@uniroma1.it
sito web: w3.uniroma1.it/sicurezza

1.INTRODUZIONE

L'enorme patrimonio culturale di cui il nostro paese dispone rappresenta una ricchezza unica a livello mondiale. La tutela di tale patrimonio richiede un totale ripensamento a tutti i livelli, in termini di sicurezza, al fine di assicurare ai beni culturali nazionali un adeguato livello di protezione.
Tale esigenza può essere soddisfatta, nella maggior parte dei casi, ricorrendo a impianti, sistemi e tecnologie di sicurezza, che entreranno sempre più a far parte nel ciclo di protezione e tutela dei beni culturali.
Gli attuali impianti di sicurezza hanno raggiunto un livello tale di funzionalità e di integrazione reciproca che è più opportuno utilizzare il termine *sistemi di sicurezza* piuttosto che il più restrittivo *impianti di sicurezza*.
Tali sistemi sono fortemente legati all'evoluzione tecnologica dell'elettronica e per tale motivo sono soggetti ad innovazioni costanti che richiedono competenze sempre più ampie in vari settori quali l'elettronica, la fisica, le telecomunicazioni, l'informatica, l'impiantistica generale, le tecnologie multimediali ed altro ancora.
Un sistema di sicurezza, per poter operare al meglio delle sue possibilità, deve essere progettato, installato, utilizzato e mantenuto con grande professionalità e competenza.
Ed è per tale motivo che i soggetti coinvolti devono possedere, a vari livelli, un elevato numero di competenze per poter ottenere dai suddetti impianti le prestazioni migliori. E' inoltre molto importante possedere una notevole esperienza pratica e diretta nel settore dei beni culturali al fine di conoscere a fondo tutte le problematiche con le quali è necessario confrontarsi ai fini della sicurezza.
In generale, ma in particolar modo nel settore dei beni culturali, gli impianti di sicurezza vengono spesso trattati senza la necessaria preparazione, lasciando ampi margini all'approssimazione e all'incompetenza, con il risultato di assistere alla realizzazione di impianti mal concepiti, che risultano essere totalmente inadeguati a fronteggiare i rischi e i pericoli concreti a cui risultano esposti i suddetti beni.
Nella lingua italiana corrente, con il termine *sistemi di sicurezza* si indicano, nella maggior parte dei casi, i sistemi rivolti alla protezione della persona fisica, dei beni materiali e immateriali non solo da attacchi volontari ma anche da eventi incidentali, quali ad esempio i sistemi di rivelazione incendi, generando talora ambiguità e incomprensioni. Tale problema non sussiste nella lingua inglese in quanto si indicano con il termine *security* i sistemi del primo tipo mentre con il termine *safety* i sistemi del secondo tipo. Tali termini tendono sempre più ad essere utilizzati anche nella lingua italiana.
I sistemi security sono per lo più rappresentati dagli impianti antintrusione e antifurto, dagli impianti di controllo accessi e dagli impianti di videosorveglianza TV a circuito chiuso (indicata brevemente come TVCC) mentre i sistemi safety sono rappresentati dagli impianti di rivelazione incendi, gas tossici e pericolosi ed altro. I sistemi security e i sistemi safety vengono integrati mediante opportune reti di trasmissioni dati e sistemi di supervisione e controllo o di building automation, dando vita a sistemi integrati di sicurezza caratterizzati da funzionalità, affidabilità e

prestazioni elevate, caratteristiche molto importanti per le complesse esigenze di protezione necessarie a garantire la sicurezza dei beni culturali.

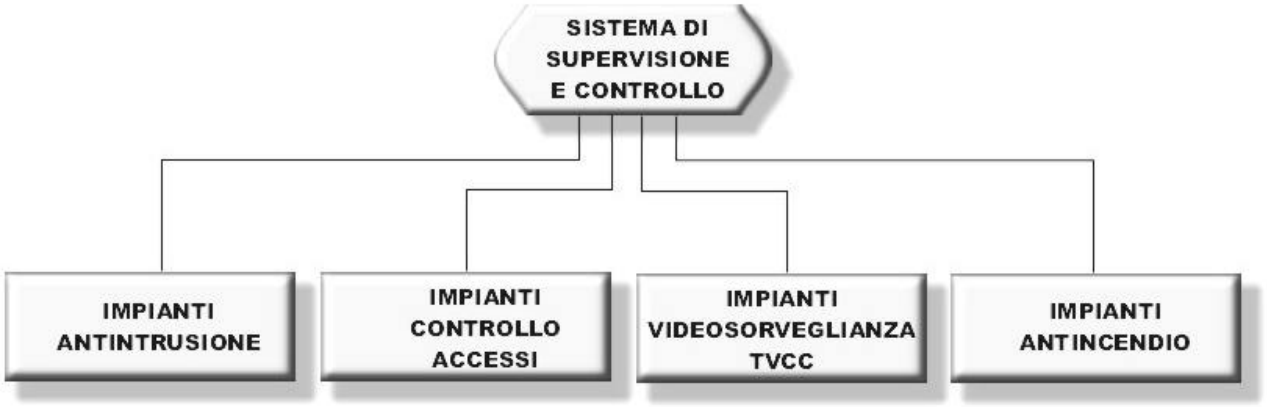


Fig.1 Schema a blocchi di un sistema di sicurezza integrato

La distinzione tra sistemi security e sistemi safety risulta essere, nella maggior parte dei casi, più formale che sostanziale. Si pensi, infatti, ad un impianto controllo accessi che blocca l'accesso in una determinata zona in cui si è verificato un incendio, o in cui è avvenuta una fuoriuscita di sostanze pericolose, proteggendo le persone da eventi incidentali pericolosi per la loro salute. Si pensi ancora al caso di un impianti di videosorveglianza TVCC, in grado di verificare la presenza di situazioni pericolose in una determinata zona, permettendo di attivare tutte le procedure necessarie alla protezione delle persone eventualmente presenti o che devono accedere in tale zona.
Qualunque tipo di sistema di sicurezza è riconducibile ad uno schema semplificato in cui sono chiaramente identificabili i seguenti componenti:
1) elementi in campo (sensori antintrusione, lettori controllo accessi, telecamere, sensori antincendio);
2) centrale di sicurezza per la ricezione, raccolta, elaborazione e gestione delle informazioni provenienti dagli elementi in campo;
3) rete di interconnessione tra elementi in campo e centrale;
4) rete di comunicazione tra la centrale e le centrali degli impianti dello stesso livello gerarchico o di livello gerarchico superiore .

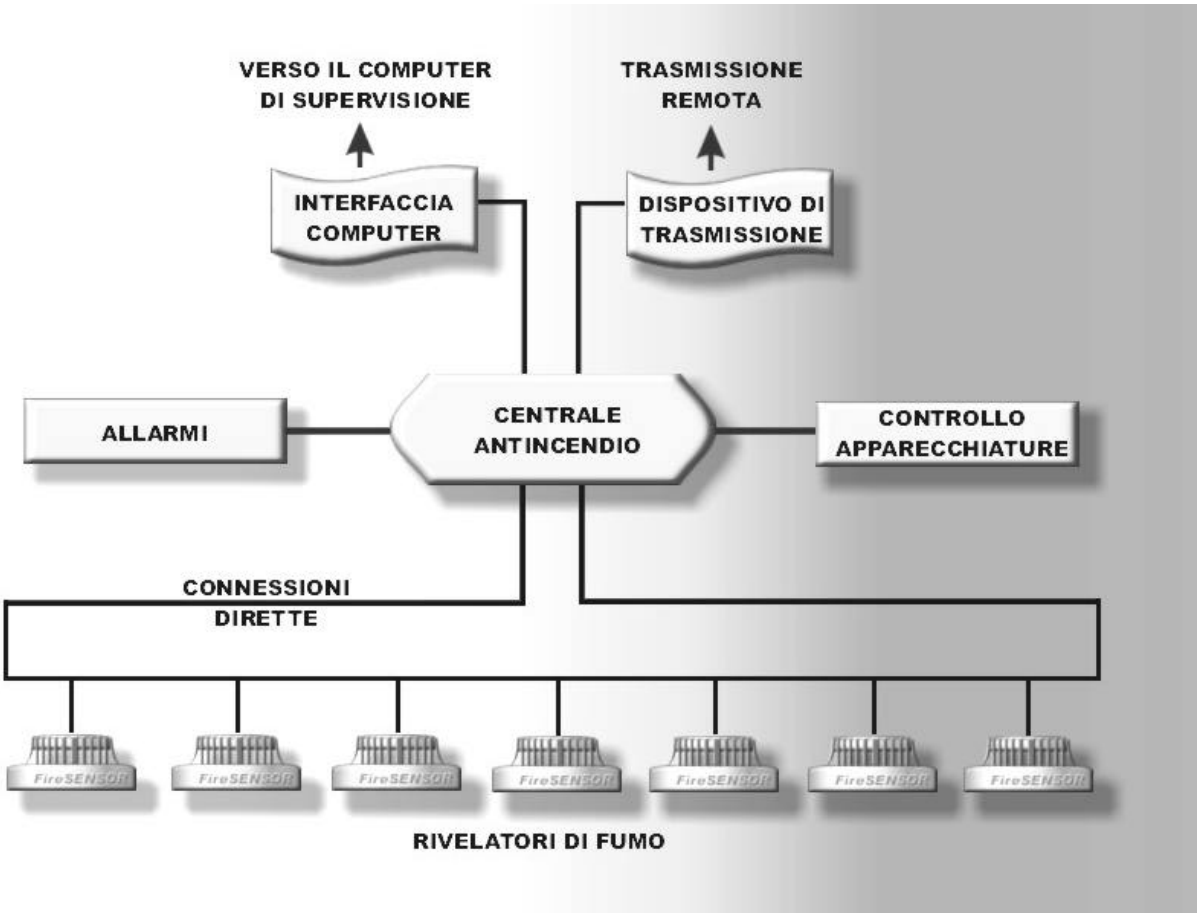


Fig.2 Schematizzazione di un sistema di rivelazione incendi. Esso può essere ricondotto allo schema generale valido per gli impianti di sicurezza, composti dai seguenti blocchi funzionali: elementi in campo, centrale di sicurezza, rete di interconnessione sensori-centrale, rete di comunicazione

Una novità molto importante per il settore dei beni culturali è rappresentata dalla possibilità di utilizzare reti di telecomunicazioni senza fili (wireless) che utilizzano la radiofrequenza per trasmettere e ricevere le informazioni, evitando il ricorso a cavi che potrebbero, in alcuni casi, non risultare estremamente gradevoli dal punto di vista estetico. E' importante ricordare che se si utilizzano, in particolare, sensori wireless, poiché questi ultimi ricorrono a batterie per il loro funzionamento, è necessario prevedere un accurato programma di sostituzione periodica al fine di evitare malfunzionamenti o spegnimenti dei sensori stessi proprio nei momenti di maggior bisogno, a causa dell'esaurimento delle batterie stesse.

Un punto fondamentale che è necessario sottolineare prima di andare avanti nella illustrazione di tali sistemi è che gli impianti, o sistemi di sicurezza, rappresentano degli strumenti fondamentali nella prevenzione e nella lotta al crimine ma hanno bisogno di operare in sinergia con opportune barriere fisiche per utilizzare al meglio le loro caratteristiche peculiari. Infatti, anche se tali impianti sono in grado di intercettare con precisione il momento e il luogo dove si verifica un'intrusione, essi non sono in grado di arrestare tale intrusione. D'altra parte nemmeno le barriere fisiche più robuste possono resistere ad attacchi di sfondamento per un tempo indeterminato. Per cui la sicurezza elettronica e la sicurezza fisica devono integrarsi fra di loro in funzione di un terzo elemento fondamentale rappresentato dall'intervento umano. Infatti se da una parte la sicurezza elettronica provvede a rivelare il tentativo o l'inizio di un attacco a fini intrusivi, dall'altra parte la sicurezza fisica deve essere in grado di garantire la resistenza delle barriere almeno fino all'intervento umano che inizia grazie alle segnalazioni degli impianti di sicurezza. La non adeguata progettazione o il non perfetto funzionamento di uno dei tre fattori suddetti implica il fallimento dell'intero piano di

sicurezza e la conseguente penetrazione all'interno dell'area protetta ove sono presenti beni culturali che, nella maggior parte dei casi, sono di valore inestimabile.

3. I SISTEMI ANTINTRUSIONE

I sistemi antintrusione rappresentano uno strumento efficiente ed affidabile per la prevenzione ed il controllo degli accessi a fini criminosi all'interno di una determinata zona.
Se essi vengono ben progettati, installati e mantenuti possono evitare che si verifichino eventi pericolosi, per le persone e i beni, quali atti di vandalismo, rapine, furti, sabotaggi ed altri eventi.
La scelta del sistema antintrusione più opportuno per una determinata applicazione non è assolutamente immediata e scontata in quanto si è già detto che ogni sito da proteggere è caratterizzato da esigenze uniche e particolari che devono essere accuratamente analizzate e soddisfatte al fine di ottenere i risultati desiderati dal sistema in considerazione.
La maggior parte della confusione riguardante tali sistemi deriva dalla varietà di metodi disponibili per la rivelazione delle intrusioni. Tali metodi possono essere combinati per dare vita ad un'infinità di soluzioni differenti che non sempre si rivelano essere adeguate per affrontare le problematiche presenti.
Spesso si usa il termine *sistemi antifurto* per indicare i sistemi *antintrusione*: tale dicitura è fortemente riduttiva in quanto i sistemi antintrusione non solo prevengono il furto in sé ma prevengono anche una serie di altri eventi ben più pericolosi del furto. Per tale motivo è più corretto utilizzare il termine *sistemi antintrusione*.

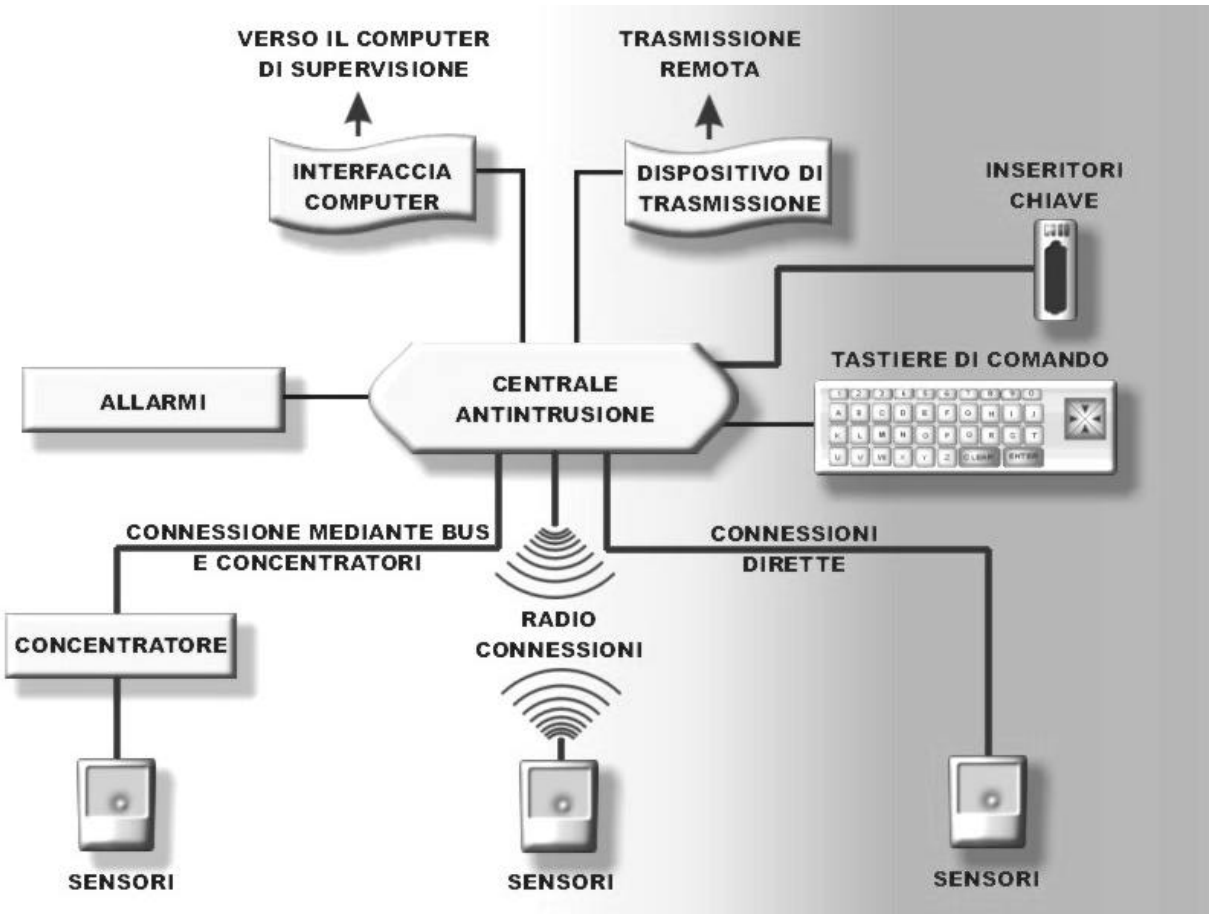


Fig.3 Schematizzazione di un impianto antintrusione

4. I SISTEMI DI CONTROLLO ACCESSI

I sistemi di controllo accessi provvedono al controllo, alla regolazione e all'organizzazione degli ingressi e delle uscite in un dato sito. Essi sono in grado di aumentare in maniera significativa e determinante la sicurezza restringendo l'ingresso solo alle persone che sono in grado dimostrare il diritto all'accesso, memorizzando opportunamente il verificarsi di tale azione.
La scelta di un sistema è un'operazione tutt'altro che semplice, in quanto ogni sito richiede un'applicazione differente e il sistema deve adattarsi all'applicazione suddetta. Quando si sceglie un sistema è molto più importante stabilire se esso sia in grado di lavorare in maniera soddisfacente per il sito in considerazione piuttosto che soffermarsi solo sulle relative funzionalità.
I sistemi di controllo accessi aumentano in maniera significativa la privacy ma non sono in grado di bloccare le persone al di fuori della zona protetta, compito che viene assegnato ai dispositivi di sicurezza fisica quali le chiusure o le barriere.
Tali impianti aumentano la sicurezza soprattutto nelle ore diurne, decidendo chi deve entrare, dove, quanto frequentemente e in quale zona protetta, ma non sono in grado di prevenire quello che avviene all'interno e sono totalmente vulnerabili alla collusione con il personale interno.
Tutti i vari tipi di sistemi utilizzano lo stesso principio che consiste nel riconoscimento di un codice opportuno o di un'altra grandezza biometrica quale il volto, l'impronta digitale, la voce o altro. Tale informazione viene acquisita dal lettore che provvede alla sua trasmissione verso l'unità di elaborazione o provvede ad una elaborazione interna, controllando se tale informazione è valida. Se l'operazione ha esito positivo il sistema invia un comando di apertura del meccanismo di chiusura che sblocca la barriera fisica e abilita l'ingresso.
La scelta di un particolare sistema avviene tenendo conto dell'ambiente in cui esso deve operare, del livello di sicurezza richiesto e delle esigenze dell'utente. Ciò è ovviamente vero per ogni prodotto ma per i sistemi di controllo accessi tali fattori debbono essere considerati con particolare attenzione.
La maggior parte dei sistemi di controllo accessi appartengono alle seguenti categorie:

1) sistemi a tastiera alfanumerica con un eventuale identificazione supplementare;
2) sistemi a carta (funzionante su effetti e principi differenti) più un eventuale codice di identificazione personale (Personal Identification Number o PIN);
3) sistemi a riconoscimento delle caratteristiche personali (biometrici).

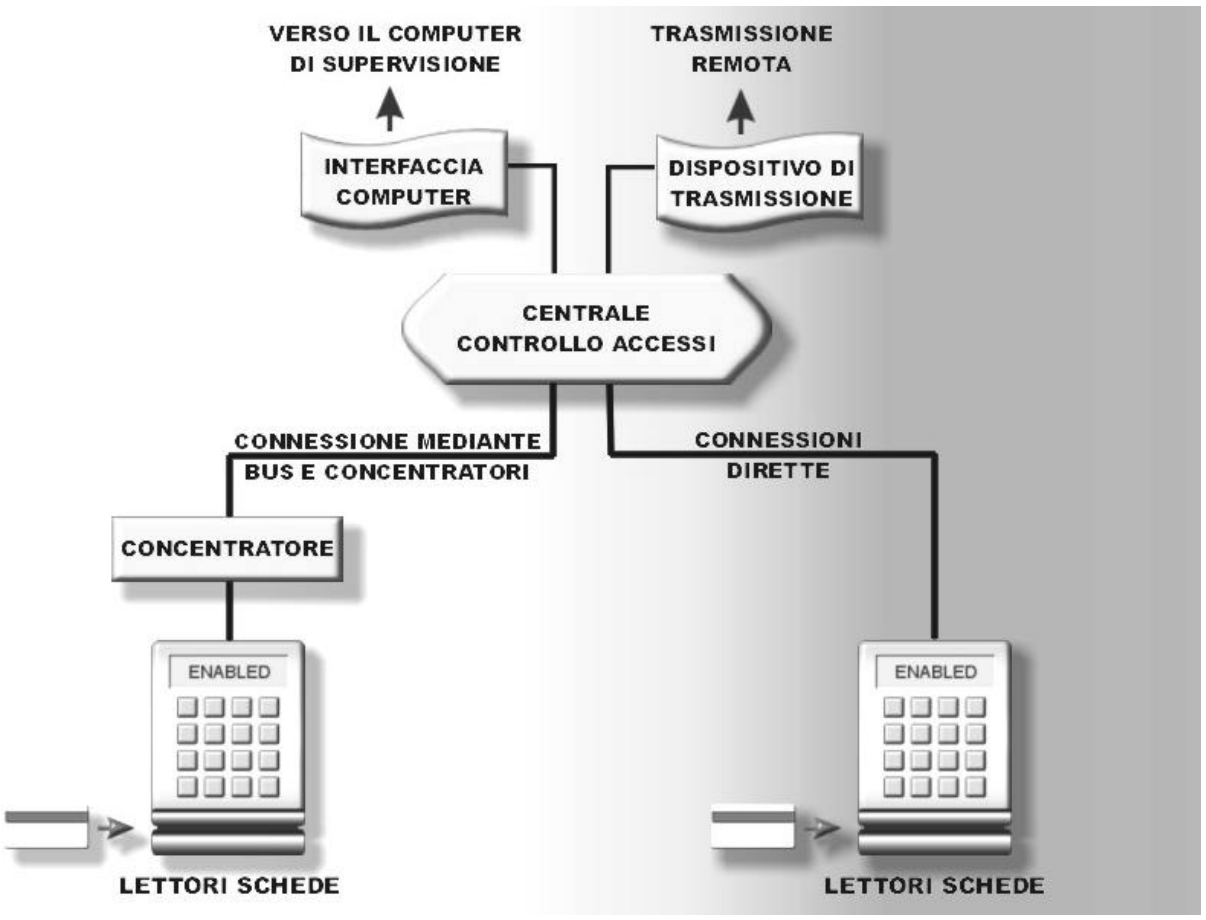


Fig.4 Schematizzazione di un impianto di controllo accessi

5. I SISTEMI DI VIDEOSORVEGLIANZA TV

I sistemi di videosorveglianza TV a circuito chiuso, denominati brevemente sistemi TVCC, rappresentano un mezzo estremamente economico e affidabile per il controllo e la prevenzione della criminalità.

Di fronte al continuo aumento del costo del lavoro e alla mancanza di risorse umane qualificate e specializzate, i sistemi TVCC rappresentano una valida soluzione ai problemi della sicurezza, riducendo drasticamente il numero di persone necessarie a fronteggiare tali problemi.

Il continuo aumento del numero dei furti e dei crimini è purtroppo un dato di fatto che riguarda ogni tipo di organizzazione, sia essa commerciale, di servizi, produttiva o statale, e soprattutto il settore dei beni culturali. Le dimensioni dell'organizzazione non costituiscono un deterrente per i malintenzionati, le cui abilità aumentano in misura diretta con le suddette dimensioni. Maggiore è il valore dei beni e la disponibilità di essi e maggiore è il rischio di attacchi criminali.

Lo scopo principale degli impianti TVCC consiste non già nel cogliere sul fatto i malintenzionati quanto nel costituire un valido deterrente contro di essi, al fine di prevenire eventuali azioni criminose.

Un malintenzionato ha bisogno di occultarsi opportunamente al fine di portare a termine la sua azione criminosa e l'impianto TVCC gioca un ruolo fondamentale nel prevenire tale occultamento, controllando accuratamente tutte le zone critiche del sito da proteggere.

Il punto di forza della TVCC è rappresentato dalla sua possibilità di integrarsi con gli altri sistemi security (antintrusione e controllo accessi) e dalla sua possibilità di poter controllare aree remote che presentano potenziali problemi di sicurezza. La TVCC si rivela anche molto utile se utilizzata insieme con i sistemi safety (per esempio rivelazione incendi), al fine di visualizzare le zone dove i sensori generano un eventuale allarme e di verificare la veridicità dell'allarme stesso.

Lo scopo della TVCC consiste, brevemente, nel fornire un occhio remoto ad un operatore di sicurezza, permettendogli di visualizzare eventi che si stanno svolgendo in tempo reale. Alcune applicazioni in cui la TVCC fornisce delle soluzioni effettive sono:

1) controllo di zone remote ai fini della sicurezza;
2) controllo simultaneo di più zone da parte di un solo operatore;
3) registrazione di eventi criminosi ai fini della produzione di prove giudiziarie.

Per utilizzare al meglio i sistemi TVCC è necessario che gli utenti finali comprendano tutti gli aspetti tecnologici che governano gli impianti suddetti, al fine di conoscerne tutti i pregi, i limiti e gli eventuali difetti.

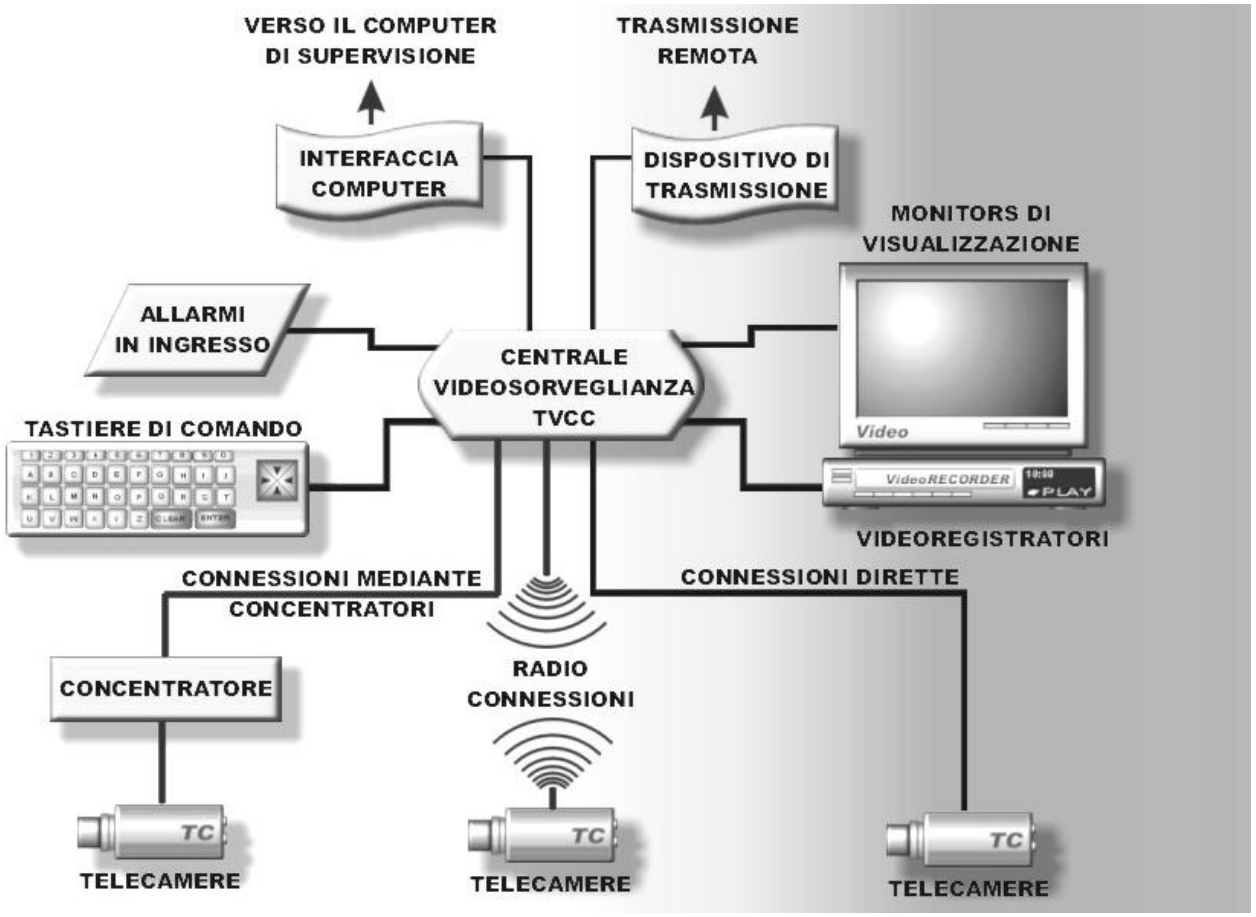


Fig.5 Schema di un sistema di videosorveglianza TVCC

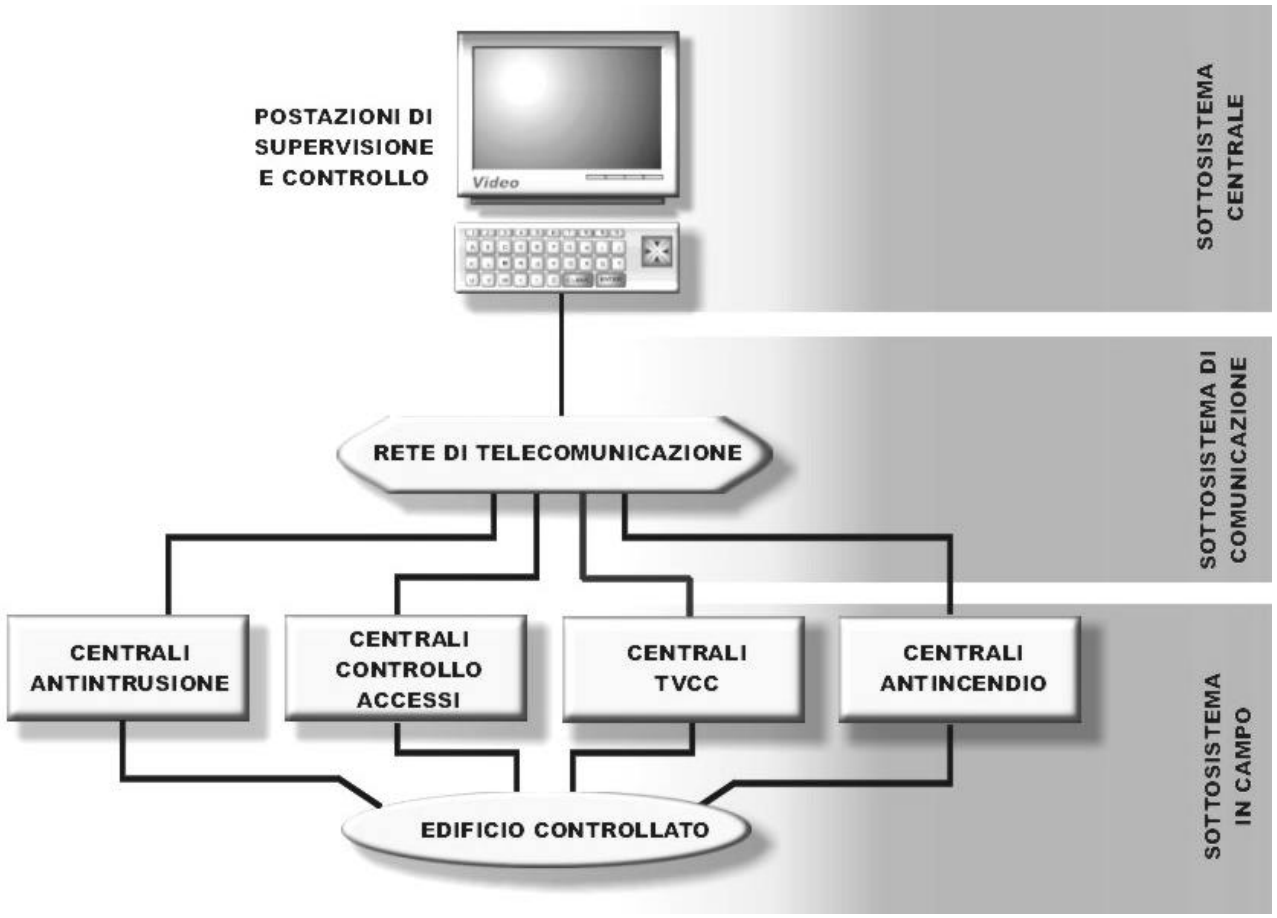
6. SISTEMI INTEGRATI DI SICUREZZA PER LA PROTEZIONE DEI BENI CULTURALI

Quando si è in presenza di un certo numero di sistemi di sicurezza per la protezione dei beni culturali, dislocati in diverse zone, non è pensabile attuare una gestione di tipo manuale per ciascuno di essi. Per tale motivo essi debbono necessariamente essere interconnessi tra di loro, dando vita a quella che viene definito un sistema integrato di sicurezza.

I sistemi integrati di sicurezza consentono la supervisione, il controllo e la gestione di uno o più impianti di sicurezza in maniera automatica e semplificata, anche se i medesimi impianti sono posti ad una notevole distanza tra di loro. Tali sistemi consentono la gestione non solo degli impianti security ma anche degli impianti safety, dando vita a sistemi integrati di sicurezza le cui funzionalità sono nettamente superiori rispetto a quelle offerte dai singoli impianti.

In realtà l'integrazione procede anche verso livelli superiori e successivi, supervisionando e controllando gli impianti di comunicazione, gli impianti tecnologici ed eventuali altri impianti e

dispositivi, dando vita alla cosiddetta automazione degli edifici (o building automation), di cui i sistemi integrati di sicurezza costituiscono una componente essenziale.
Essi permettono di accentrare in una o più postazioni le segnalazioni di allarme generate dai vari impianti, unificando le procedure di gestione, ottimizzando le necessità di risorse di personale di sicurezza e la manutenzione.
La corretta integrazione dei sistemi di sicurezza deve essere perseguita coordinando la progettazione degli impianti con le esigenza del personale di sicurezza e con adeguate procedure di gestione, migliorando l'utilizzo dei singoli componenti al fine di utilizzare pienamente le loro caratteristiche funzionali.
E' sempre importante ricordare che quando si procede all'integrazione del sistema, si debbono tenere in considerazione due fattori fondamentali rappresentati dalle caratteristiche dell'utilizzatore finale e dall'affidabilità del sistema stesso.
Spesso si assiste a sistemi caratterizzati da elevata complessità che non vengono integrati con un corretto sistema di elaborazione e gestione delle informazioni, saturando il livello di corretta ricezione dell'utilizzatore finale con una serie di allarmi, informazioni e segnalazioni che inducono inevitabilmente uno stato di inadeguatezza e di elevato stress nelle persone deputate alla gestione del sistema stesso. Un sistema integrato, in quanto tale, deve possedere una serie di filtri e procedure interne che automaticamente attuano i programmi più opportuni in funzione degli allarmi in corso, richiedendo l'intervento dell'utente finale solo nei casi strettamente necessari, senza richiedere a quest'ultimo conoscenze tecniche particolari.
Analogamente si assiste a sistemi integrati la cui funzionalità e le cui prestazioni decadono a seguito del cedimento di un singolo componente di basso livello, quale una comune porta di comunicazione seriale, attraverso cui vengono incautamente eseguite delle operazioni vitali per il sistema stesso.
L'architettura generale di un sistema integrato di sicurezza è sostanzialmente riconducibile a tre elementi fondamentali: l'impiantistica specifica in campo, la rete di telecomunicazione ed il sistema centrale.



I sistemi integrati di sicurezza per la protezione dei beni culturali, Ambiente&Sicurezza, IL SOLE 24ORE, Giugno 2003

Fig.6 Architettura generale di un sistema di sicurezza integrata

7. CONCLUSIONI

Da quanto si è visto sinora è immediato dedurre che per garantire la protezione dei beni culturali, ricorrendo ai sistemi di sicurezza, è importante agire con competenza e preparazione, acquisendo preliminarmente una profonda conoscenza del bene da proteggere. Infatti un approccio non corretto non solo non è in grado di assicurare la protezione del bene stesso ma può addirittura compromettere, in maniera permanente, la sua integrità e fruibilità a causa di possibili danneggiamenti o furti.